REMARKS

The comments of the applicant below are each preceded by related comments of the examiner (in small, bold type).

3. Claim 6 objected to because of the following informalities: Claim 6 is mistakenly marked as currently amended when it appears no changes have been made. Appropriate correction is required.

Claim 6 has been amended.

5. Claim 40 rejected under 35 U.S.C. 102(e) as being anticipated by Lyle, U.S. Patent No. 6,886,102.

As per claim 40:

Lyle discloses a method comprising:

At a server, receiving from at least two remote clients indications of possible security problems at the clients (6:52-7: 18); and

Determining in real time at the server an existence of an anomaly based on the indications of the possible security problems from the at least two remote client locations (6:52-7:18)

6. Claims 1-3, 6-8, 9-11 and 14-22 and 28-34 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (Shostack), U.S. Patent No. 6,298,445 in view of Lyle, U.S. Patent No. 6,886,102.

As per claim 1:

Shostack discloses a method comprising:

detecting a possible security problem at a client location (6:43-46, wherein an intrusion is a possible security problem);

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the location (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server);

determining at the home location an anomaly based on at least the possible security problem 7:15-16, wherein the security vulnerabilities function as anomalies and the local server is the home location); and

transmitting notice of the anomaly in real time to the client location (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach determining at the home location an anomaly based on information sent to the home location from at least one other client location and transmitting notice of the anomaly to the client location at which the possible security problem is detected. However, Lyle discloses a method wherein an event, which consists of an actual or suspected attack, is determined based on information gleaned from an internal source called a sniffer (6:52-7: 18). Lyle also discloses a method wherein the responsive action, such as a message is sent to the device with the actual or suspected attack (8:21-59).

Lyle does not disclose or suggest sending in real time, from the server to the remote clients, information for updating firewalls protecting the remote clients to account for the anomaly, in which the anomaly is determined in real time at the server based on the indications of possible security problems from at least two remote client locations, as recited in amended claim 40.

Lyle discloses routers having firewall functionality (col. 6, lines 40-41), but does not disclose or suggest sending in real time information for updating firewalls to account for an anomaly determined in real time based on the indications of possible security problems from at least two remote client locations. Similarly, Shostack discloses a firewall 12 (col. 4, lines 23-25) but lacks the features recited in claim 40.

Claims 1, 9, 17, 28, 30, 41, and 42 are patentable for at least similar reasons as claim 40.

As per claim 41 :
Shostack discloses a method comprising:
detecting a possible security problem at a client location (6:43-46, wherein an intrusion is a possible security problem);
transmitting notice of the possible security problem across a network in real time to a home location remotely located from the location (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server);
transmitting notice of the anomaly in real time to the client location (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).
Shostack fails to teach determining at the home location an anomaly based on the possible security problem by searching for particular information in the anomaly. However, Lyle discloses searching for a particular file type associated with a known intrusion technique (10:44-59).

Shostack and Lyle do not disclose or suggest determining an anomaly by searching for particular information in the anomaly, the particular information including at least one of "a network address previously noted as a security problem and a particular query or command associated with a known intrusion pattern or technique," as recited in amended claim 41.

Although Lyle discloses a sniffer module that detects whether a particular port is receiving a high number of packets with a certain target destination or recipient address (col. 10, lines 44-49), Lyle does not disclose or suggest searching for a network address previously noted as a security problem.

As per claim 42:

Shostack discloses a method comprising:

detecting a possible security problem at a client location (6:43-46, wherein an intrusion is a possible security problem);

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the location (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server);

transmitting notice of the anomaly in real time to the client location (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach determining at the home location an anomaly by at least comparing the possible security problem with information previously logged at the home location. However, Lyle discloses a method wherein the event, which consists of an attack, is compared to other events that have occurred (7:50-8:11) .

...

Claims 43 and 44 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack (U.S. 6,298,445) in view of Lyle (U.S. 6,886,102) as applied to claims 42 above and further in view of Moran, U.S. Patent No. 6,826,697.

As per claims 43 and 44:

Shostack and Lyle fail to teach a method in which determining the anomaly comprises searching for non-standard access patterns such as a login from an unexpected user. However, Moran discloses a method wherein failed login attempts are logged (19:41-20:18). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle with Moran because in order to make a system less vulnerable to attack as stated in Shostack (2:18-28) the ability to detect further types of attacks such as forward and backward time steps in a log file or an overflow buffer attack as stated in Moran (4:1-37) would increase the security against attacks as a whole.

Moran does not disclose or suggest "searching for an unexpected login," as recited in amended claim 42.

The "login" recited in claim 42 is a successful login, not a failed login. By contrast, Moran discloses logging of "failed" login attempts. Moran does not disclose or suggest searching for an unexpected login.

All of the dependent claims are patentable for at least the same reasons as the claims on which they depend.

Canceled claims, if any, have been canceled without prejudice.

Any circumstance in which the applicant has addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner. Any circumstance in which the applicant has made arguments for the patentability of some claims does not mean that

there are not other good reasons for patentability of those claims and other claims. Any circumstance in which the applicant has amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

Please apply any charges or credits to deposit account 06-1050, reference attorney docket 10559-463001.

Respectfully submitted,

Date: 3/2/2006

Rex Huang

Rex L. Huang
Reg. No. 57,661

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21239022.doc